5.8.9 Malware Prevention Policy

Chapter 5 - Information Technology	Original Effective Date: June 2003
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: October 2016

I. Purpose

To establish the standard for protecting information resources from threats posed by malware.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. General

UT Health San Antonio Information Resources and network infrastructure must be continuously protected from threats posed by Malware. All computing devices must be configured with an approved Malware protection software and configuration that is defined to detect and clean Malware that may infect the device or data it holds or accesses.

1. All computing devices owned, leased or under the control of UT Health San Antonio (UTHSA) must, to the extent technology permits, execute and keep up to date Malware protection software and adhere to any other Malware prevention and protection measures as required by UT Health San Antonio policies, standards and procedures.
2. The Malware protection software must not be disabled or bypassed, its frequency of updates, modified or its configuration altered to an operating state that no longer meets UTHSA policies and standards.

3. Verification of Malware protection software configuration signature files or engine files will be performed by a centralized anti-malware administration system, or through other information security monitoring practices.
4. Use of Malware protection not defined in UTHSA policies or standards must be approved as an exemption by the Chief Information Security Officer (CISO).
5. Malware not discovered by Malware protection software or configuration controls is considered a security incident and must be reported to the Chief Information Security Officer.

B. Email Malware Protection

All email gateways must execute and keep up to date Malware protection software and adhere to any other prevention and protection measures as required by UTHSA policies, standards and procedures.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

UT System (UTS) Policy

UTS 165 Information Resources Use and Security Standard 8: Malware Prevention

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2003	Policy Origination		
10/2016	Policy Revision		
02/2023	Policy Review/Discretionary Edits		